AMENDMENTS TO THE CLAIMS

Claims 1-23 (Canceled)

Claim 24 (Previously Presented): A method performed by a machine comprising:

receiving a user password;

receiving a user identification;

receiving a plurality of names for independent software applications that require a password for a user to use any of the software applications;

generating a unique and specific randomly generated salt value for each independent software application;

computing a software application dependent password for a user for a selected independent software application, wherein the software application dependent password only depends on the user password, the user identification and the specific randomly generated salt value associated with the selected software application; and

returning the software application dependent password for the selected independent software application to the user,

wherein a user does not need to one of remember the selected software application dependent password and record the selected software application dependent password as the software application dependent password is one of computed each time a user requests access to the software application and temporarily stored a first time the user requests access to the software application for a predetermined time period.

Claim 25 (Canceled)

Claim 26 (Previously Presented): The method of claim 24, wherein the computation of the software application dependent password further includes hashing the user name, the user password, and the salt value for the software application.

Claim 27 (Previously Presented): The method of claim 24, further comprising generating an old password if the old password is required.

Claim 28 (Previously Presented): The method of claim 24, wherein a strong password is used to generate a plurality of software application passwords.

Claim 29 (Canceled)

Claim 30 (Currently Amended): A method performed by a machine comprising:

receiving a plurality of names for independent software applications that require a password for a user to use any of the software applications;

generating a plurality of random salt values for each ~~a plurality of~~ software applications;

generating a hash from ~~a~~ one random salt value and input data, the one salt value only associated with one specific software application, the input data including a user identification and a strong password;

generating a software application dependent password from the hash; and

returning the software application dependent password to a user to gain entry to the software application,

wherein a user does not need to one of remember the software application dependent password and record the software application dependent password as the software application dependent password is one of computed each time a user requests access to the specific software application and temporarily stored a first time the user requests access to the specific software application for a predetermined time period.

Claim 31 (Previously Presented): The method of claim 30, further comprising:

receiving the input data;

determining if the salt value exists;

generating the salt value and storing the salt value in a table entry if the salt value does not exist; and

retrieving the salt value from the table entry if the salt value exists.

Claim 32 (Canceled)

Claim 33 (Previously Presented): The method of claim 30, wherein the input data further comprises a software application identification.

Claim 34 (Previously Presented): The method of claim 30, further comprising determining if a new strong password is required; and

retrieving the new strong password if the new strong password is required.

Claim 35 (Previously Presented): The method of claim 30, wherein the strong password is used to generate a plurality of software application passwords.

Claim 36 (Previously Presented): The method of claim 30, wherein the salt value is one of predetermined and generated by a random number generator.

Claim 37 (Previously Presented): The method of claim 30, wherein the salt value and the software application are associated in the table entry.

Claim 38 (Previously Presented): The method of claim 30, wherein the software application is run on one of a local computer system and a networked computer system.

Claim 39 (Previously Presented): The method of claim 30, wherein one of a secure hash algorithm (SHA-1) and a message digest (MD5) algorithm are used to generate the hash.

Claim 40 (Previously Presented): The method of claim 30, wherein the generated password is temporarily stored in a memory for a predetermined time period.

Claim 41 (Previously Presented): The method of claim 40, wherein the predetermined time period is based on platform activity.

Claim 42 (Previously Presented): The method of claim 41, wherein the platform is one of a local computer system and a networked computer system.

Claim 43 (Currently Amended): A program storage device readable by a machine comprising instructions that cause the machine to:

receive a plurality of names for independent software applications that require a password for a user to use any of the software applications;

generate~~ing~~ a plurality of random salt values for ~~a plurality of~~the software applications;

generate a hash ~~from~~ for each of the plurality of random salt values and input data, each salt value only associated with one specific software application, the input data including a user identification and a strong password;

generate a software application dependent password ~~from~~ for ~~the~~ one hash for a user selected software application; and

return the software application dependent password to a user for the selected software application to gain entry to the selected software application,

wherein the user does not need to one of remember the software application dependent password for the selected software application and record the software application dependent password for the selected software application as the software application dependent password is generated each time a user requests access to the ~~specific~~ selected software application.

Claim 44 (Previously Presented): The program storage device of claim 43, further comprises instructions that cause the machine to:

receive input data;

determine if a salt value exists;

generate a salt value and store the salt value in a table entry if the salt value does not exist; and

retrieve the salt value from the table entry if the salt value exists;

Claim 45 (Canceled)

Claim 46 (Previously Presented): The program storage device of claim 43, wherein the input data further comprises a software application identification.

Claim 47 (Previously Presented): The program storage device of claim 43, further comprises instructions that cause the machine to:

determine if a new strong password is required; and

retrieve the new strong password if the new strong password is required.

Claim 48 (Previously Presented): The program storage device of claim 47, wherein the strong password is used by the machine to generate a plurality of software application passwords.

Claim 49 (Previously Presented): The program storage device of claim 43, wherein the salt value is one of predetermined and generated by a random number generator.

Claim 50 (Previously Presented): The program storage device of claim 43, wherein the salt value and the software application are associated in the table entry.

Claim 51 (Previously Presented): The program storage device of claim 43, wherein one of a secure hash algorithm (SHA-1) and a message digest (MD5) algorithm are used in instructions to cause the machine to generate the hash.

Claim 52 (Previously Presented): The program storage device of claim 43, wherein the generated password is temporarily stored in a memory for a predetermined time period.

Claim 53 (Previously Presented): The program storage device of claim 52, wherein the predetermined time period is based on platform activity.

Claim 54 (Previously Presented): The program storage device of claim 52, wherein the platform is one of a local computer system and a networked computer system.